



QUALYS SECURITY CONFERENCE 2019

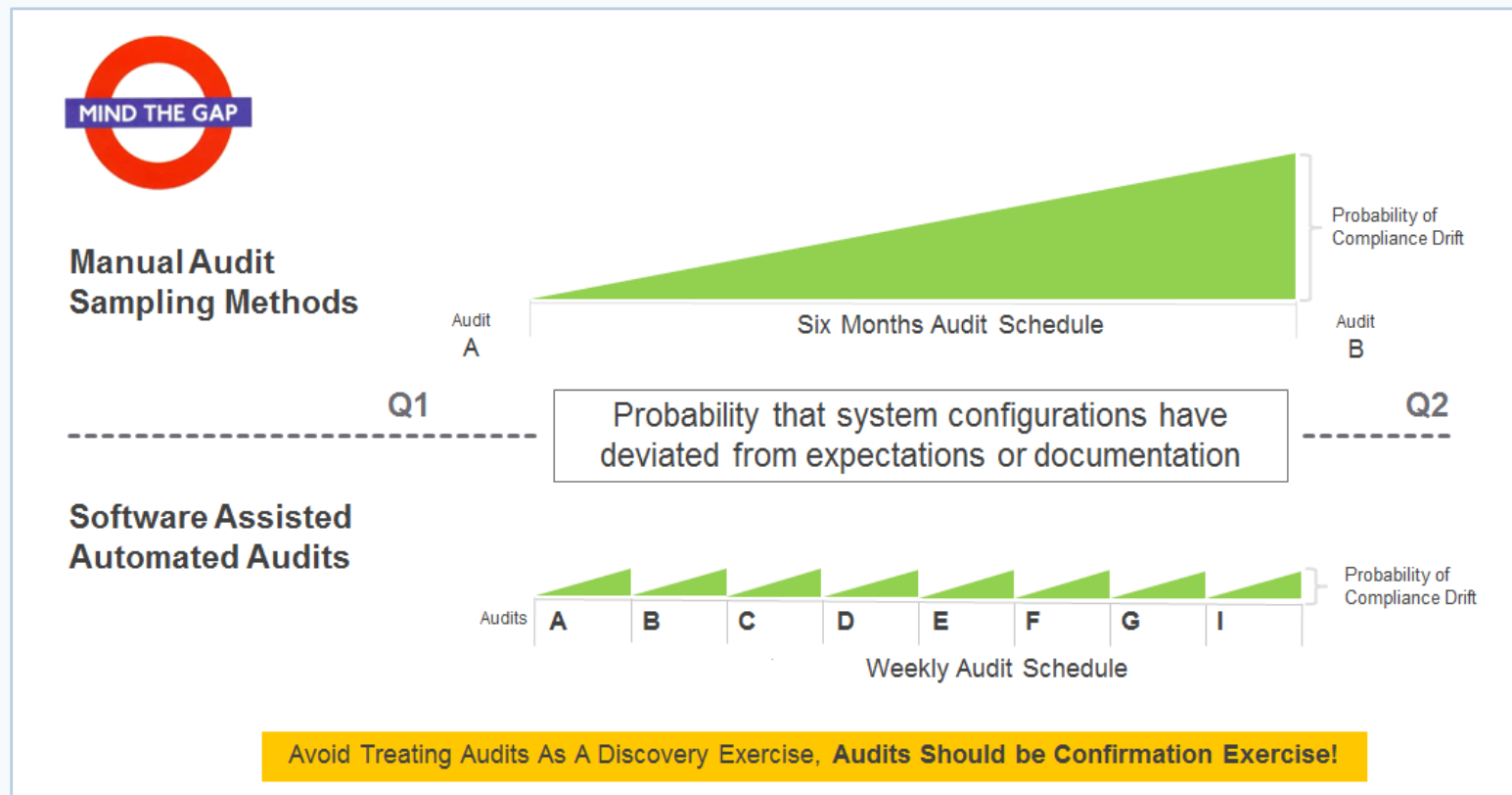
# Continuous Compliance in Hybrid Environment

New Frontier in Unified Compliance, Configuration  
and File Integrity Management

**Shailesh Athalye**

VP, Compliance Solutions, Qualys, Inc.

# 2014: Good Old Days of Compliance



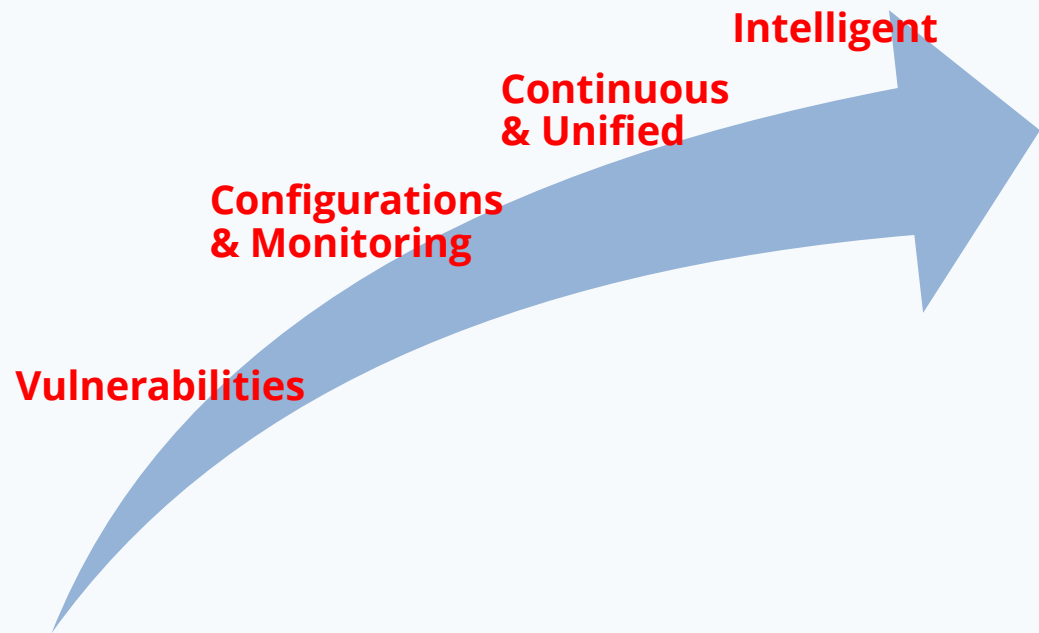
# 2019: Security is Continuous and Unified

To reduce the 'attack surface'

To reduce breaches due to misconfigurations, lack of monitoring

## **Question remains:**

Is Compliance and Risk really continuous?



# Compliance and Risk are Not Connected with Security

Section of HIPAA Security Rule	HIPAA Security Rule Standards	Implementation Specifications
164.308(a)(5)(i)(D)		Password Management (A): Procedures for creating, changing, and safeguarding passwords.

Part	Applicable Systems	Requirements
5.5	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA  Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters:  5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and  5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber

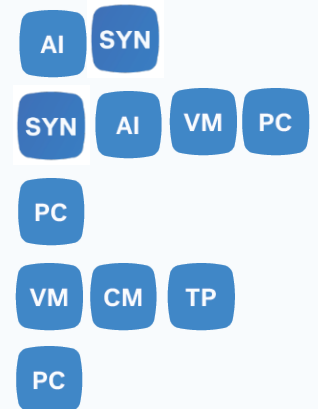
ISO/IEC 27001 (Annex A) CONTROLS
A.11.2 User access management
A.11.2.1 User registration
A.11.2.2 Privilege management
A.11.2.3 User password management

CSC 16-3	Ensure that systems automatically create a report that includes a list of locked-out accounts, disabled accounts, accounts with passwords that exceed the maximum password age, and accounts with passwords that never expire. This list should be sent to the associated system administrator in a secure fashion.
----------	---



Inventory Your Systems  
Inventory and Restrict Software  
Secure Configurations  
Continuous VM



# Semi-automated Way for Connecting

Time to value

Time to see roll up the operational data

Security data of varied nature

FIM, Patch, Malware

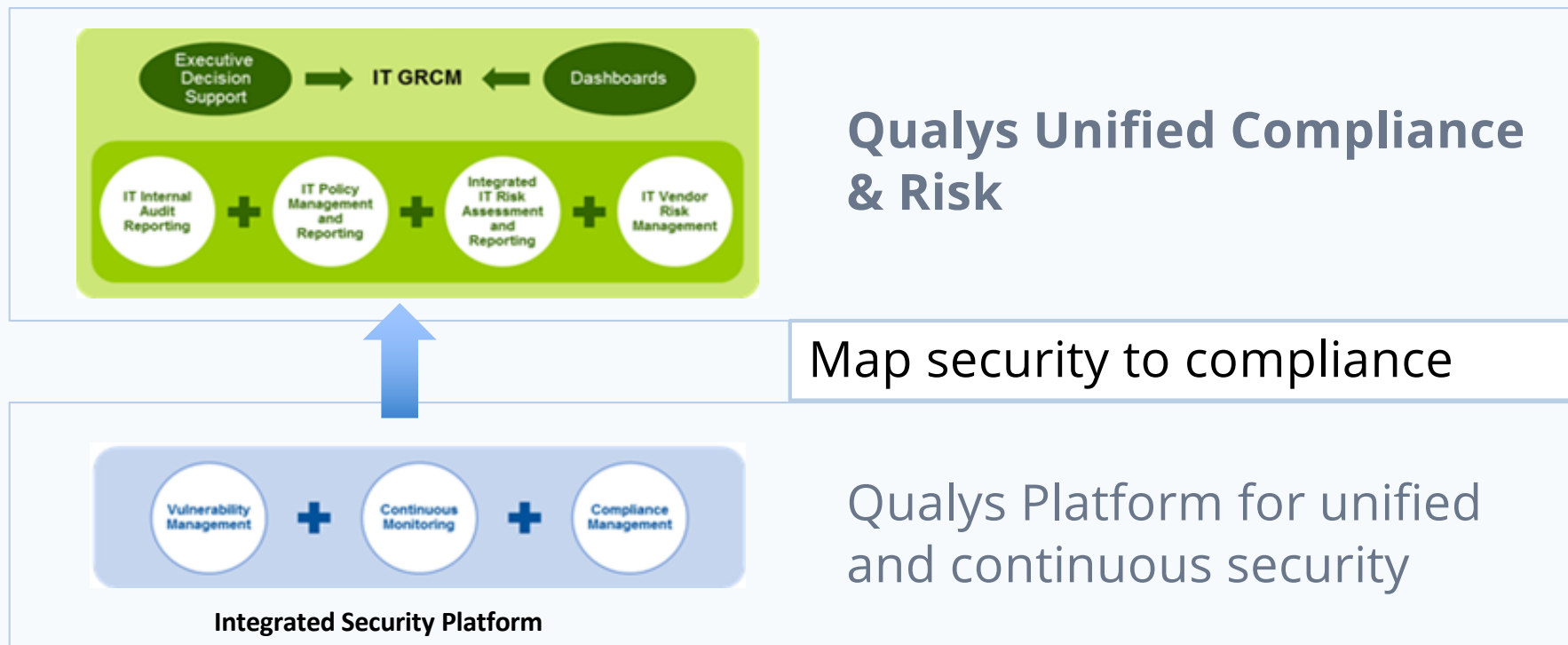
Scoping and Tracking 'In-Scope'

Assets

Application complexity with connectors



# Continuous Compliance & Risk From Continuous Security



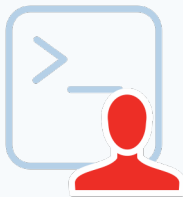
# Continuous Compliance from Continuous Security

Qualys Unified Compliance maps every app's output to compliance requirements

The screenshot displays the Qualys Unified Compliance Assessment interface. The top navigation bar includes links for HOME, DASHBOARD, ASSESSMENT (active), REPORTS, and CONFIGURATION. Below this, a secondary navigation bar shows Mandates, Assessment (active), Risk, and Tickets. A search bar at the top of the main content area contains the query 'Mandate.name like %Fedramp Mod%' and a filter for 'Last 30 days'. Four summary cards are displayed: TOTAL CONTROL OBJECTIVE (325), FAILED CONTROL OBJECTIVE (98), TOTAL CONTROLS EVALUATED (223K), and FAILED CONTROL EVALUATIONS (26K). Below these cards, there are buttons for 'Action' and 'Generate Report', and a pagination indicator showing '1 - 10 of 325'. The main table lists assessment results for Mandate ID IA-5, titled 'Authenticator management'. The table has columns for MANDATE ID, OBJECTIVE, OBJECTS, POSTURE EVALUATION (STATUS, PASS, FAIL), ASGNT.STATUS, and CRITICALITY. The table is expanded to show details for IA-5 (1) Password-Based Authentication, which includes sub-sections for Datacenter Assets, SaaS Objects, Mobile Devices, and Public Cloud Services. Each sub-section lists specific controls with their CIDs, control names, object counts, posture evaluation status, and criticality.

MANDATE ID	OBJECTIVE	OBJECTS	STATUS	PASS	FAIL	ASGNT.STATUS	CRITICALITY
IA-5	Authenticator management	1992	Fail	1036	959	-	Critical
IA-5 (1)	Password-Based Authentication	1308 (Assets)	Fail	1011	297	-	Critical
	Datacenter Assets	1134 (Assets)	Fail	907	227	-	NA
	CID	CONTROL NAME	OBJECTS	POSTURE EVALUATION			CRITICALITY
	1071	Status of minimum password strength	1058 (Assets)	Fail	838	220	Unassigned Critical
	10459	Status of required special characters	824 (Assets)	Fail	634	190	Unassigned Critical
	SaaS Objects	1 (Connector)	Pass	1	0	-	NA
	CID	CONTROL NAME	OBJECTS	POSTURE EVALUATION			CRITICALITY
	60032	GSUITE Admin Strong Password Policy...	1 (Connectors)	Pass	1	0	Resolved Critical
	61011	Microsoft365 AD Password Policy Enforc...	1 (Connectors)	Pass	1	0	Resolved Critical
	Mobile Devices	170 (Assets)	Fail	100	70	-	NA
	CID	CONTROL NAME	OBJECTS	POSTURE EVALUATION			CRITICALITY
	89	Mobile phone passcode length	170 (Assets)	Fail	100	70	In Progress Critical
	Public Cloud Services	3 (Connectors)	Pass	3	0	-	NA
	CID	CONTROL NAME	OBJECTS	POSTURE EVALUATION			CRITICALITY
	6	Ensure that AWS IAM password policy is ...	3 (Connectors)	Pass	3	0	NA Critical
	7	Ensure IAM password policy requires at ...	3 (Connectors)	Pass	3	0	NA Critical

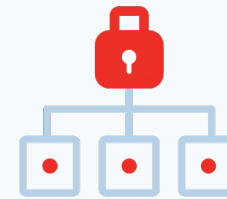
# New-age Challenges: Teams Speaking Different Languages



Elastic, Kafka, custom  
web servers



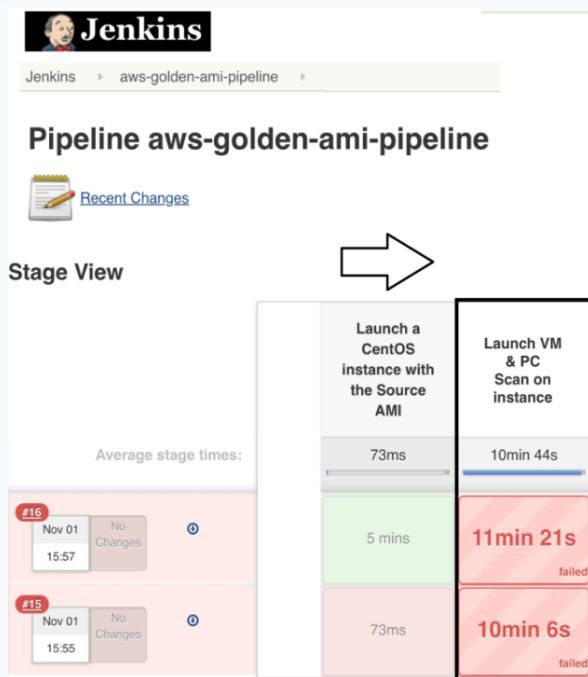
Identify risk and  
compliance



Secure hosts, config/integrity/  
vulnerability management

Security & Compliance needs should be running with DevOps from the start

# Start Compliant, Stay Compliant in DevOps with Qualys PC

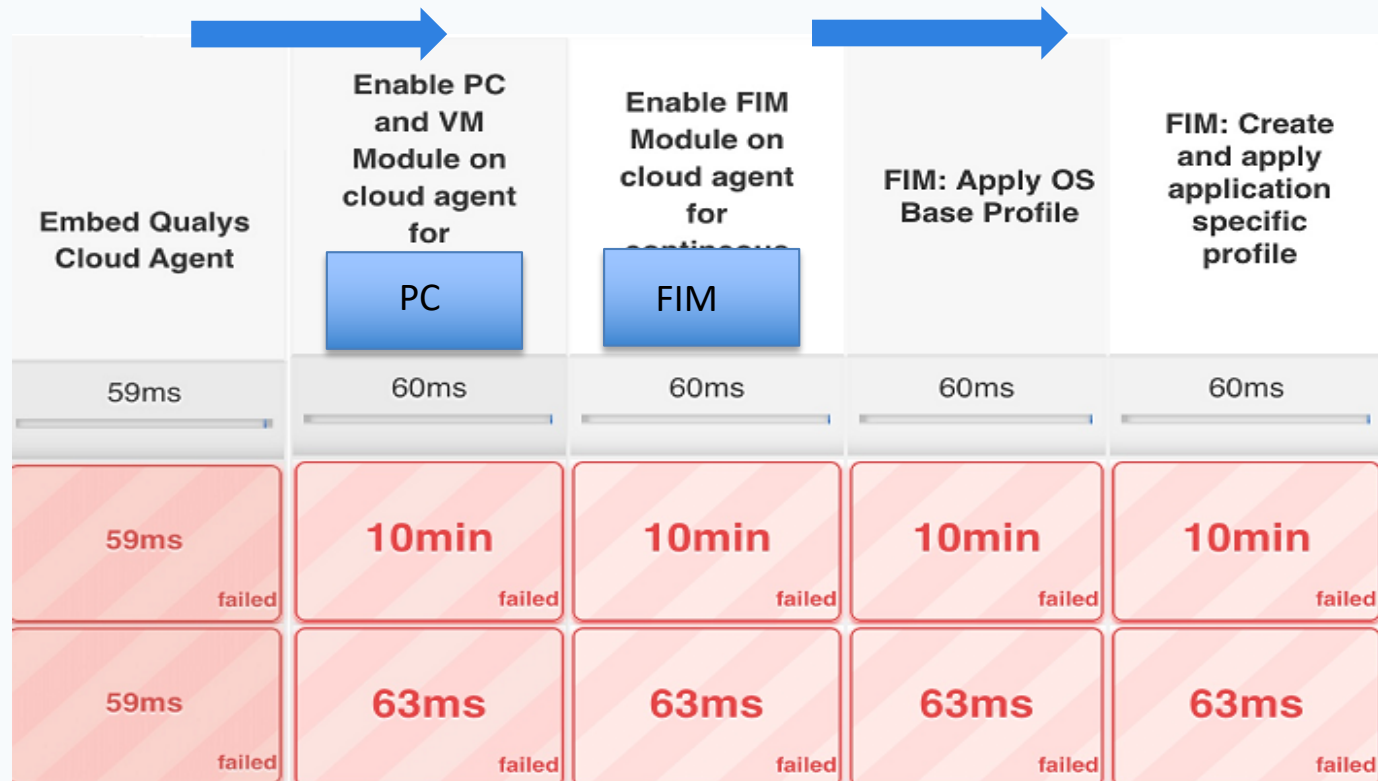


## QUALYS POLICY COMPLIANCE RESULTS

Show 10 entries

CID	Title	Technology	Criticality
14602	Status of the 'nosuid' option for '/tmp' partition using 'mount' command	CentOS 7	4
10804	Status of the SELinux current mode (running configuration)	CentOS 7	4
10643	Status of iptables package	CentOS 7	4
12815	List of runtime audit rules for '/etc/passwd' file, using auditctl	CentOS 7	4
10664	Status of the 'OPTIONS' setting within '/etc/sysconfig/chronyd' file	CentOS 7	4
9473	Existence of the 'extraneous' files and directories (Sensitive files/Directories)	Tomcat 8	3
9477	Status of 'X-Powered-By' setting within 'server.xml' file	Tomcat 8	4
9551	Status of the 'secure' attribute for each 'Connector' elements whose 'SSL Enabled' are set to 'true'	Tomcat 8	4
9605	Status of the command-line flag 'STRICT_SERVLET_COMPLIANCE' set for the Tomcat process	CentOS 7	4
9565	Status of the 'web server processes' which are not started with 'Security Manager'	CentOS 7	4

# Qualys FIM Monitors From CD Phase





## CISO Responsibility: Ensure Security Controls are in Place and Functioning <https://www.bitsight.com/blog/ciso-roles-and-responsibilities>

Is Anti-virus active, updated for signatures, scanning?

Is FIM, EDR agent configured correctly to monitor?

Are OS native application protection, memory protection configured?

Need to have Security Control Validation (SCV) in place test and confirm that security tools configured properly on all endpoints

# Security Control Validation from Policy Compliance

Anti-virus technologies | Qualys FIM Agent | Splunk | Kafka | Native Malware Protection

Reports		Control View				
51 Total Control Instances		<input type="text" value="pc.policy.name: 'Qualys Security windows' and pc.control.category: 'Anti-Virus/Malware'"/>				
CATEGORY Anti-Virus/Malwa... 51		1 - 50 of 51				
CRITICALITY MEDIUM 3 SERIOUS 18 CRITICAL 26 URGENT 4		STATUS	CID	CONTROL	TECHNOLOGY/INSTANCE	ASSET NAME
POSTURE PASS 41 ERROR 1 FAIL 9		Nov 13, 2019			os	10.10.36.125   COMDEV
		PASS	12364	Status of the 'CommunicationStatus' (Last time st	Windows 10	comqaw10es
		Nov 13, 2019			os	10.10.36.126   COMQAV
		PASS	12364	Status of the 'CommunicationStatus' (Last time st	Windows Server 2012 R2	i-6f91d2a8
		Nov 13, 2019			os	10.11.114.112   I-6F91D
		PASS	13738	Status of the Symantec 'last Virus scan time' older	Windows 2008 Server	com-2k8-32-87
		Nov 13, 2019			os	10.10.32.87   COM-2K8-
		PASS	13738	Status of the Symantec 'last Virus scan time' older	Windows 10	comdevw10es
		Nov 13, 2019			os	10.10.36.125   COMDEV
		Qualys Policy for Security Control Validation on Windows Platform				
		PASS	13738	Status of the Symantec 'last Virus scan time' older	Windows 10	comqaw10es
		Nov 13, 2019			os	10.10.36.126   COMQAV

# Start Gold, Continuously Assess, Remediate

Policy Compliance ▾ DASHBOARD POLICIES SCANS **REPORTS** EXCEPTIONS ASSETS USERS

Reports Reports Schedules Policy Summary **Control View** Templates Setup

72  
Total Controls

LABELS  
Qualys 72

TAGS  
USproduction 72

Policy.name like '%RDP%' and asset.tagName='USproduction' and control.status='failed' Last 24 Hrs ▾

Display: Unified Control Asset

CONTROL COMPLIANCE Policy.name like '% RDP%'

100%

06

● Failing

TRENDING

10  
5  
0

Jan 01 TODAY

1 - 50 of 75

Actions Group by...

Create Remediation Job

Create Alert

Add Exception

		CONTROL NAME	TECHNOLOGY	ASSET NAME	POLICY EVALUATION
<input checked="" type="checkbox"/>		Status of the 'Terminal Services' service	Windows 2008 Server	XAVIERHQ39WIN 10.10.31.30	Jun 02, 2018
<input checked="" type="checkbox"/>	Failed Mar 21, 2018	Status of the 'Terminal Services' service	Windows 7	SFO03HQLP79 10.10.35.242	Mar 21, 2018
<input checked="" type="checkbox"/>	Failed Jun 02, 2017	Status of the 'Set time limit for active Remote Desktop Services sessions' setting	Windows 10	SFO04HQLP713 10.10.35.241	May 03, 2018
<input checked="" type="checkbox"/>	Failed	Current list of Groups and User Accounts granted the	Windows	DC03SJC1SQLDB	Oct 22, 2018

# Alert and Incident Management for Authorized vs Unauthorized Changes During Patching

Qualys. Enterprise

File Integrity Monitoring ▾

DASHBOARD EVENTS **RULES** INCIDENTS REPORTS ASSETS CONFIGURATION

Activity Rule Manager Actions

3  
Total Activities

ruleName: "Unauthorized Windows Patching Activity" or ruleName: "Authorized Windows Patching Activity" Last 30 Days ▾

14 Oct 16 Oct 18 Oct 20 Oct 22 Oct 24 Oct 26 Oct 28 Oct 30 Oct 1 Nov 3 Nov 5 Nov 7 Nov 9 Nov 11 Nov 13 Nov 15 Nov

1 - 3 of 3

RULE NAME	STATUS ▾	AGGREGATE	ACTION	MATCHES	CREATED BY
<b>Authorized Windows Patching Activity</b> Authorized Windows Patching Activity	Success 29 minutes ago	Yes	Windows Patch Activity...	1	Aparna Hinge
<b>Unauthorized Windows Patching Activity</b> Unauthorized Windows Patching Activity	Success 29 minutes ago	Yes	Windows Patch Activity...	1	Aparna Hinge
<b>Unauthorized Windows Patching Activity</b> This Rule lists down all the events which ...	Success 2 hours ago	Yes	Windows Patch Activity...	1	Aparna Hinge

**RULE NAME**

- Unauthorized Wi... 2
- Authorized Wind... 1

**ACTION NAME**

- Windows Patch ... 3

**EMAIL RECIPIENTS**

- ljhamb@qualys.c... 3
- akaur@qualys.co... 3
- shin@qualys.co... 2

# FIM gives context of changes in cloud

Qualys Enterprise

← Asset Details : i-076e2369b896dfe3e

## INVENTORY

Asset Summary  
System Information  
Network Information  
Open Ports  
Traffic Summary  
Cloud Information

## SECURITY

Vulnerabilities  
Threat Protection  
Patch Management  
Indication of Compromise  
Certificates  
Secure Access Control  
SOAR

## COMPLIANCE

Policy Compliance  
File Integrity Monitoring

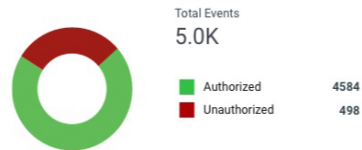
## SENSORS

Agent Summary  
Connector Summary  
Passive Sensor  
Alert Notifications

## File Integrity Monitoring

Cloud Agent FIM Events S3 FIM Events

UNAUTHORIZED EVENTS ON S3 BUCKET FROM INSTANCE (INSTANCE ID)



TIME	TARGET	ACTION	ACTOR	EVENT STATUS	SEVERITY
an hour ago 12:08:18 PM	bucketauditreports/ 636123215182/us-west-1	PutBucketPolicy	InstanceProfile/i-07f6... assumed-role	Access	
an hour ago 12:08:18 PM	bucketauditreports/t... 636123215182/us-west-1	GetObject	InstanceProfile/i-07f6... assumed-role	Access	
an hour ago 12:08:18 PM	bucketauditreports/ec2... 636123215182/us-east-1	DeleteObject	InstanceProfile/i-07f6... assumed-role	Unauthor	
an hour ago 12:08:18 PM	bucketauditreports/RDS... 636123215182/us-west-1	DeleteObject	InstanceProfile/i-07f6... assumed-role	Unauthor	
an hour ago 12:08:18 PM	bucketauditreports/tom... 636123215182/us-west-1	DeleteObject	InstanceProfile/i-07f6... assumed-role	Unauthor	

# Network Devices Can't be Scanned or Hosts too Sensitive but in Security & Compliance Scope

Use OCA APIs

- Create custom assets
- Push command output, vulnerability, config data

Controls validate settings

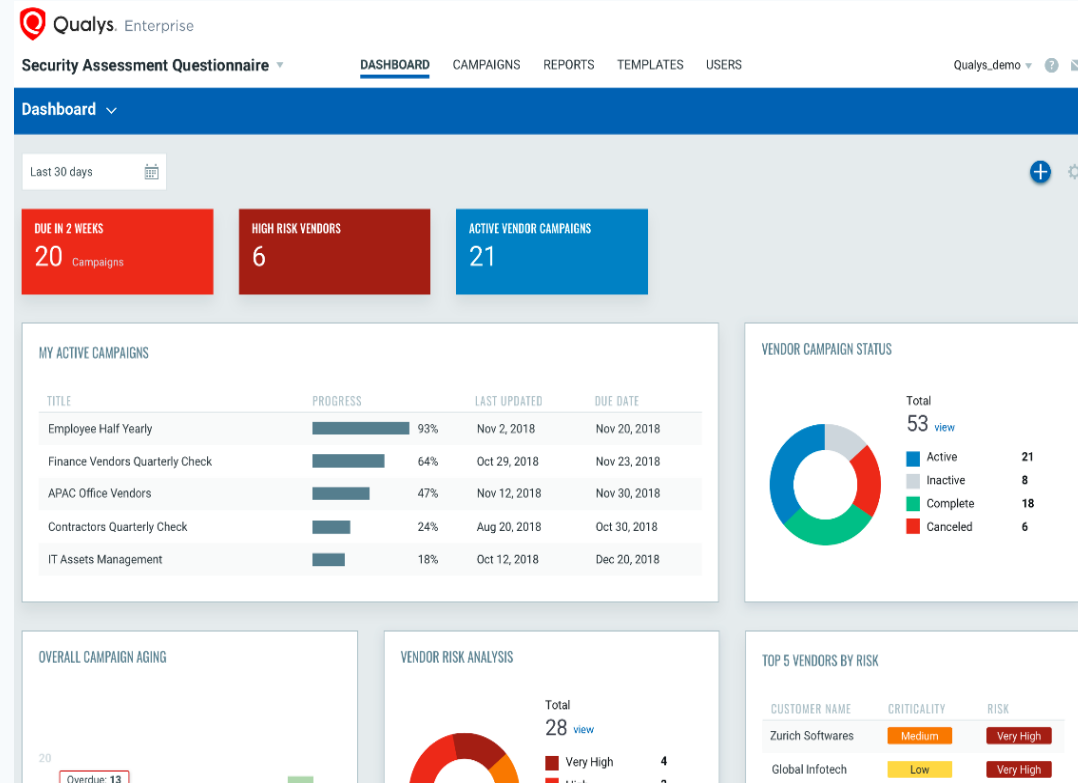
Report vulnerabilities, security and misconfigurations

The screenshot displays the HP FutureSmart 4.x interface showing detailed scan results for the IP address 154.36.214.3 (hp-in01-prn02, HP-IN01-PRN02). The interface includes a header with the HP logo and a menu bar (File, View, Help). Below the header, the 'Detailed Results' section shows the target IP and a summary of controls: 12 total, 12 passed (100%), 0 failed, 0 errors, 0 approved exceptions, and 0 pending exceptions. A 'Collapse All' link is also present. The main content area is titled 'HP FutureSmart 4.x' and lists various system configuration checks under the heading '1. System Configuration'. Each check is accompanied by a severity level (CRITICAL, SERIOUS, or PASS) and a status (PASS or FAIL).

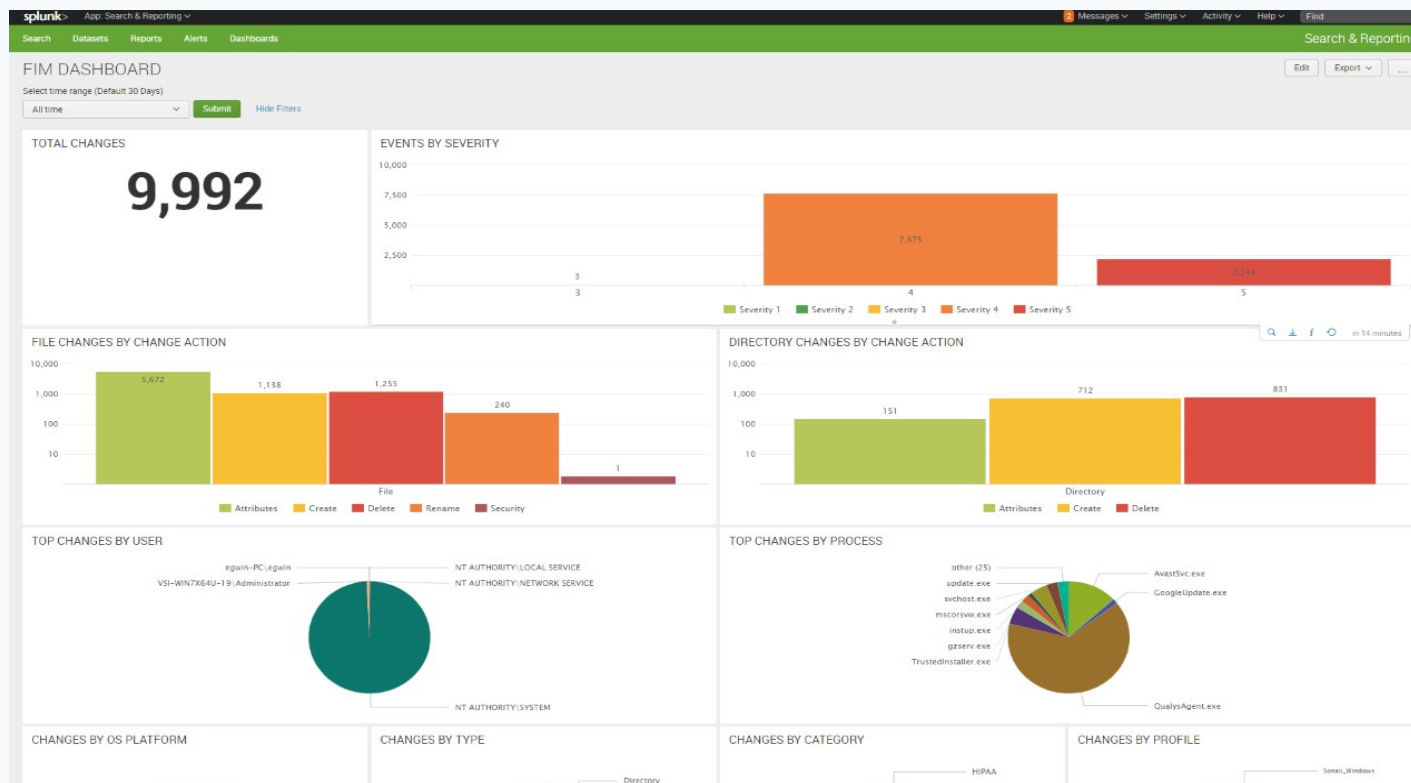
Check ID	Description	Severity	Status
(1.1) 1116	Status of the 'File Transfer Protocol (FTP)' service	CRITICAL	PASS
(1.2) 1861	Status of the 'telnet' service	CRITICAL	FAIL
(1.3) 10270	Status of the SNMP community strings	SERIOUS	PASS
(1.4) 12413	Status of the 'AppleTalk' protocol	SERIOUS	PASS
(1.5) 13857	Status of version of firmware stored in boot PROM	CRITICAL	PASS
(1.6) 14039	Status of SNMP configuration of version SNMPv1	CRITICAL	PASS

# Your security is only as strong as your weakest vendor

Qualys Security Assessment Questionnaire (SAQ) helps in managing vendor risk per criticality



# Open APIs: Integrate with Any External SIEM, DWH



The background is a solid blue color with a pattern of small white dots arranged in a grid. Three red dots are scattered on the background: one in the upper right, one in the lower left, and one in the middle left.

# Policy Compliance (PC)

# Policy Compliance Advantages

Best in class technology and content coverage  
For Configuration Management

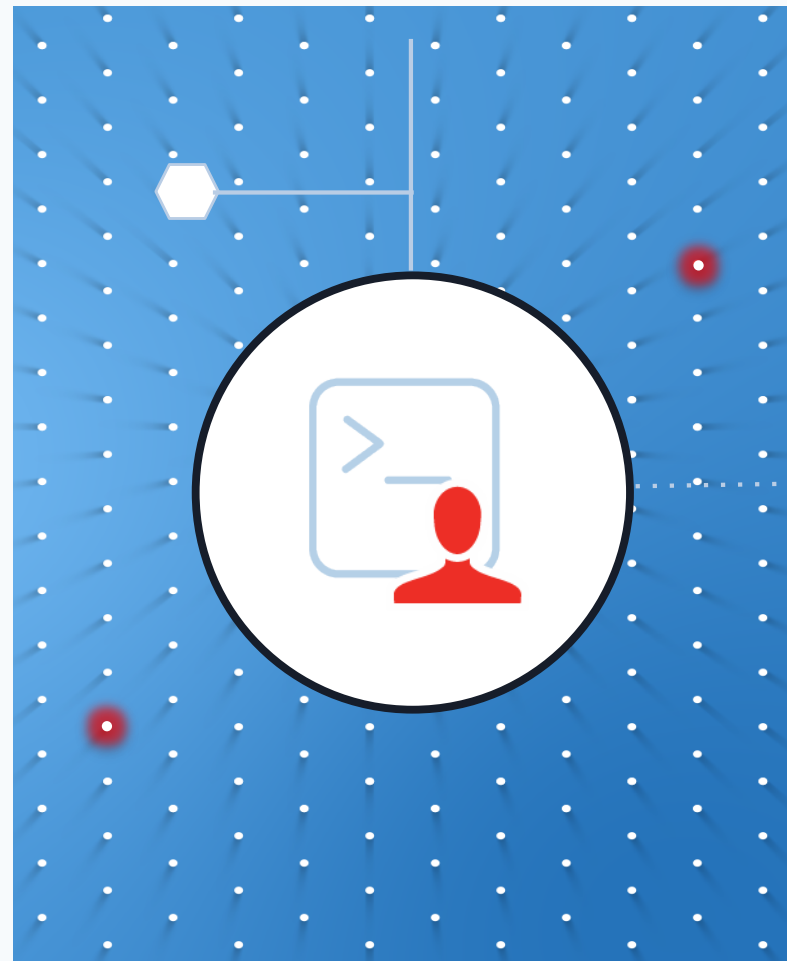
- >400 Policies, >10,000 controls
- >150 technologies (traditional, emerging)
- > Widest coverage for CIS, STIG, Mandates and beyond


Data collection from all Qualys sensors

Custom database security & integrity controls

Auto-discovery of middleware technologies

Auto-remediation for configuration failures



The background is a solid blue rectangle. Overlaid on this is a grid of small white dots, arranged in a pattern that is denser towards the corners. Three red dots with a soft, glowing aura are positioned at specific points: one in the upper-left area, one in the lower-right area, and one on the right edge, slightly above the center.

# New PC UI and Customizable Dashboard

# PC Roadmap

## Q4 - 2018

Faster PC agent data processing  
File Content search for Windows  
(Search sensitive content)  
Auto-discovery for database techs

## Q4 - 2018

New, customizable PC dashboard

## 2020 Q1

New PC UI  
Dynamic, real-time compliance against policies, mandates  
Integration of PC/config data with Asset Inventory  
Gold policies to fix configuration Issue 'upfront'  
Ticketing integration with JIRA, ServiceNOW

## 2020 Q2

Configuration assessment for RDS  
Automated alerting for compliance, config failures  
Support for executing scripts/commands for custom apps  
PC agent support for web server technologies  
Compliance trending



# File Integrity Monitoring (FIM)

# Qualys FIM: In First Year

Built on the same Qualys Cloud Agent

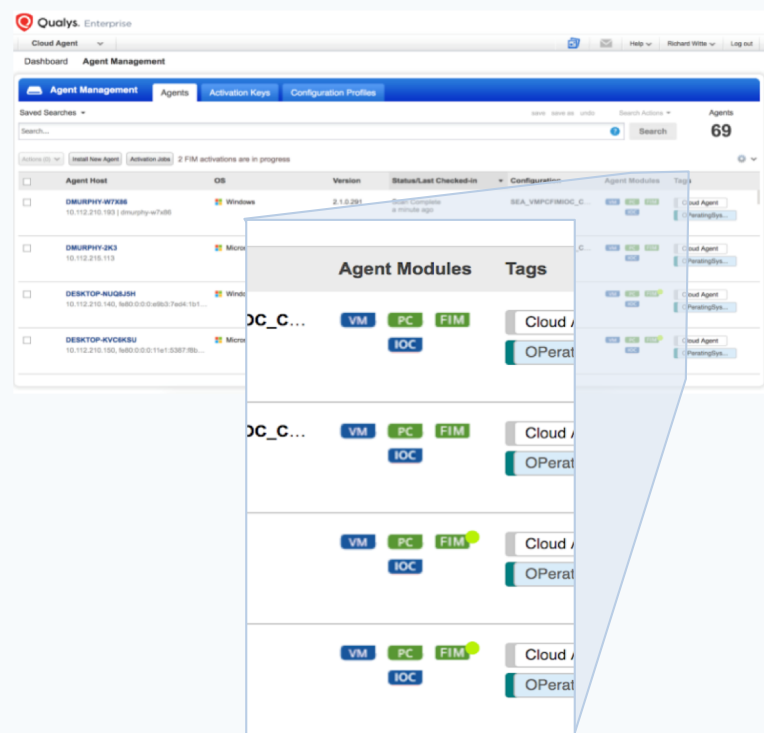
Real-time detection for high volume, high scale

Nothing to install, easy to configure, quick win

Automated incident management and alerting

Out of the box PCI monitoring profiles for OS and applications

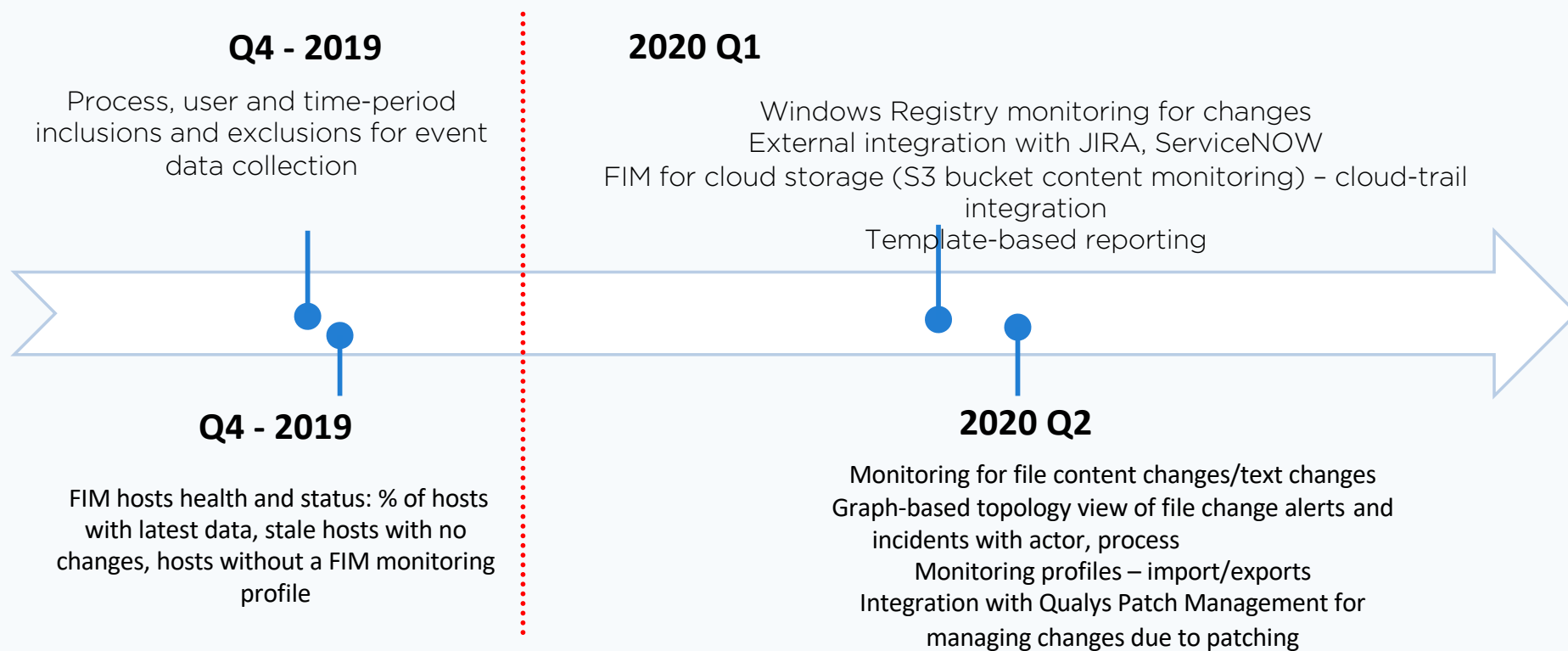
No infrastructure, data load for you to manage



The image features a solid blue background. Overlaid on this background is a vector field represented by a grid of small white arrows. These arrows are arranged in a pattern that suggests a flow or field, with their orientation varying across the space. Three specific points within this field are highlighted with red dots, each having a soft, circular glow around it. One red dot is located in the upper right quadrant, another in the lower left quadrant, and the third is positioned towards the middle left. The word "Demo" is centered in the image in a white, sans-serif font.

Demo

# FIM Roadmap





QUALYS SECURITY CONFERENCE 2019

# Thank You

Compliance Team and Shailesh Athalye  
[sathalye@qualys.com](mailto:sathalye@qualys.com)